Dynamic, Cooperating Boundary Controllers

Intrusion Response in Networked Systems

3. Containment

2. Tracking

4. Reporting
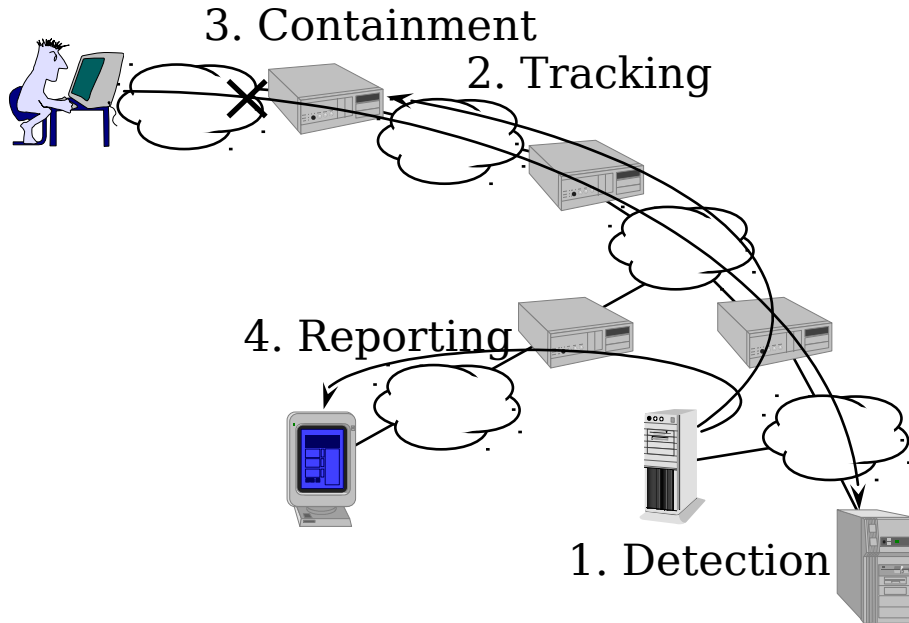
1. Detection

NEW IDEAS

- Concept of operation that enables intrusion detection and access control devices to cooperate in intruder detection, tracking, and containment

- Intruder Detection and Isolation Protocol (IDIP) to integrate heterogeneous, autonomous components

- Support for network management to provide centralized monitoring and control of intruder response

IMPACT

- Improved survivability to network-based attacks

- Improved protection from insider attacks

- Support for network-wide intrusion response

SCHEDULE

Protocol Interoperability Demonstration

Final Report

1996	1997	1998

Protocol Design Complete

Proof of Concept Demonstration